patent application Ser. No. 08/853,955, a fingerprint can be used to generate secure PIN data. In FIG. **5**, module **200** includes a fingerprint-sensitive screen **320** upon which a user during a transaction places a fingerprint **330**. Such screens typically are charge sensitive, but may be implemented in other ways as well. Unit **250** with software **35** and/or **45** examines the pattern of a central portion of fingerprint **330**, and by executing an algorithm determines a token or PIN value. This token PIN is substantially unique to fingerprint **330**, and it is extremely unlikely that the pattern of a fingerprint of another user attempting to use card **230** would generate the same PIN token.

The token PIN can earlier have been stored in card **230** (magnetically in stripe **220** and/or in memory **225** if card **230** is a smartcard), for example when the card was issued. Further, remote host system **75** can also have been provided with the token PIN value at the time of card issuance. If the transaction-generated fingerprint token PIN value agrees with the known token PIN value (obtained from card **230** and/or remote host system **75**), the transaction is allowed to proceed. It will be appreciated that among the advantages of a fingerprint token PIN value are the extremely secure and substantially non-duplicable nature of this PIN, and the fact that the card user no longer has to memorize a PIN value for use during a transaction. Further, it may be advantageous not to encrypt the token PIN value within card **230** or host system **75**, due to the inability of a person other than the card owner to generate a fingerprint token PIN value with module **200** during a transaction.

FIG. **6** depicts an embodiment in which module **200** further includes a signature capture unit **255**. In this embodiment, unit **255** includes a pressure sensitive screen **340** upon which a signature or other writing **350** may be drawn with a stylus **360**. In the embodiment shown, unit **255** includes a preferably LCD unit immediately beneath the pressure sensitive surface of screen **340**. The result is that as the tip of stylus **360** is moved across the surface of screen **340**, pixels in the writing **350** are displayed.

Electronics within unit **355** in conjunction with software **35** and/or **45** captures, signal processes, and preferably compresses signature **350**. The compressed signature data may then be transmitted by unit **10** to remote host system **75**, which stores a valid exemplar of the signature of the true owner of card **230**. If the host system stored signature matches the module **200** written signature, the host system will return a signal, visible and/or audible, to device **10** whereupon the transaction will be allowed to complete.

The embodiment of FIG. **7** provides module **200** with a smartcard reader/writer unit **255**, as well as with a pressure sensitive screen **340**. It is understood that unit **255** could of course be provided in any of the embodiments of FIGS. **2**–**6** in addition to or in lieu of magnetic card stripe reader unit **210**. In FIG. **7**, screen **340** and electronics **255'** need not display screen pixels touched by the tip of stylus **360**. In the embodiment shown, a virtual pinpad **370** is displayed on screen **340** and is responsive to pressure from the tip of the stylus. A user may manually enter a PIN by touching various of the keys displayed on screen **340** with the stylus tip or other object.

Memory **225** within smartcard **230** can store substantially more data than can one or even three magnetic stripes. An appropriate smartcard **230** may store user account number, present maximum dollar limit of the account, user identification as well as preferably encrypted PIN data. Generally when a user purchases a smartcard **230**, memory **225** is programmed to store the dollar value of the card, e.g., the

value of the card. In a preferred embodiment, smartcard reader/writer unit **260** can both read and write to memory **225**. Thus, if prior to the present transaction memory **225** stored $1,000 as the present card balance and if the present transaction is a $200 debit, unit **260** can so debit memory **225** such that the new present card balance is $800.

As noted, according to the present invention, module **200** may include any or all combination(s) of magnetic stripe reader unit **210**, smartcard reader/writer unit **260**, pinpad unit **240**, printer unit **245**, fingerprint unit **250**, and signature capture unit **255**. It will be appreciated that the present invention may be marketed as modular kit, including an assembly of these modules, or modules including two or more of these units. The kit could also include appropriate software **35**/**45** storable in device **10** memory for execution by CPU **20**.

Modifications and variations may be made to the disclosed embodiments without departing from the subject and spirit of the invention as defined by the following claims.

What is claimed is:

1. For use with a computer device that includes a central processor unit (CPU), memory, and a PCMCIA-complaint card slot connector, and for use with a card bearing magnetically stored information, a portable point of sale transaction module comprising:

a module housing including a projecting member having a PCMCIA-compliant connector sized to matingly engage said card slot connector in said computer device;

a virtual pinpad unit, disposed in said housing, including a screen upon which a pinpad image responsive to user contact-entry during said transaction is displayed; and

a card reader able to read data stored on a card in a manner selected from a group consisting of (i) data stored magnetically on at least one magnetic stripe on said card, and (ii) data stored in a solid state memory contained within said card, said card reader disposed in said module housing;

wherein software storable in said memory and executed by said CPU processes data read from said card by said card reader during a transaction made with said card and processed pinpad data entered by said user on said virtual pinpad, including user-entered personal identification number data entered during said transaction.

2. The portable point of sale transaction module of claim **1**, wherein said card reader is a magnetic stripe reader, and said card is a credit card.

3. The portable point of sale transaction module of claim **1**, wherein said card reader includes a smartcard reader/writer, and said card is a smartcard.

4. The portable point of sale transaction module of claim **1**, wherein said computer device is selected from a group consisting of (i) a personal digital assistant (PDA), and (ii) a laptop computer.

5. The portable point of sale transaction module of claim **1**, wherein an owner of said card has a personal identification number (PIN) that must be correctly manually entered on said pinpad unit during said transaction to complete said transaction.

6. The portable point of sale transaction module of claim **1**, wherein said module includes software and memory storing encryption keys to encrypt PIN data manually entered on said pinpad unit during said transaction, such that said PIN is not made available to said device except in encrypted form, to promote security.

7. The portable point of sale transaction module of claim **1**, wherein an owner of said card has a personal identifica-